Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Please amend claim 30 as indicated below. Material to be inserted is in **bold and underline**, and material to be deleted is in ~~strikeout~~ or (if the deletion is of five or fewer consecutive characters or would be difficult to see) in double brackets [[ ]].

Listing of Claims:

1. (Previously Presented) A method for regulating the ability of a sender to print on a printer, comprising the steps of:

receiving, at a printer, a print job from a sender, where the print job includes a representation of a document and an aspect of the print job that is encrypted with a private key of the sender;

verifying the sender by decoding the aspect using a public key of the sender, where the public key and the private key form a key pair; and

printing the document on the printer only if the aspect of the print job is decoded successfully.

2. (Previously Presented) The method of claim 1, where the printer is located at a printing site and printing is contingent on re-verification of the sender at the printing site.

3. (Previously Presented) The method of claim 2, where re-verification includes demonstrating possession of the private key by the sender at the printing site.

4. (Original) The method of claim 3, where the private key is stored on a portable processor and possession is demonstrated with a locally-restricted optical signal.

5. (Original) The method of claim 1, where the aspect relates to content of the print job.

6. (Original) The method of claim 1, where the aspect, after encryption, is a digital signature.

7. (Original) The method of claim 1, where the public key is included in a digital certificate.

8. (Original) The method of claim 1, where the public key is included in the print job.

9. (Original) The method of claim 1, where the public key is obtained by the printer from a public key database.

10. (Previously Presented) The method of claim 1, where the public key is linked to an authorization table that permits the sender to print on the printer.

11. (Previously Presented) The method of claim 1, where the print job is at least partially encrypted by the sender with a public key of the printer.

12. (Previously Presented) A system for regulating the ability of a sender to print on a printer, comprising:

a sending processor that includes a private key of a sender, where the private key forms a key pair with a public key, the sending processor being adapted to encrypt an aspect of a print job using the private key and to send the print job and encrypted aspect over a network; and a printer in communication with the sending processor, where the printer is adapted to receive the print job and encrypted aspect from the sending processor, to verify the sender by decoding the encrypted aspect using the public key, and to print a document based on the print job only if the aspect of the print job is decoded successfully.

13. (Previously Presented) The system of claim 12, where the printer is located at a printing site and the sender is verified upon a demonstration that the sender possesses the private key at the printing site.

14. (Original) The system of claim 12, further including a portable processor that stores the private key in memory and carries out the demonstration.

15. (Original) The system of claim 12, where the aspect relates to content of the print job.

16. (Original) The system of claim 12, where the aspect, after encryption, is a digital signature.

17. (Original) The system of claim 12, where the public key is included in a digital certificate.

18. (Original) The system of claim 12, where the public key is included in the print job.

19. (Original) The system of claim 12, where the public key is obtained by the printer from a public key database.

20. (Previously Presented) The system of claim 12, where the public key is linked to an authorization table that permits the sender to print on the printer.

21. (Original) The system of claim 12, where the print job is at least partially encrypted with a public key of the printer.

22. (Previously Presented) A printer capable of regulating output of a print job from a sender, comprising:

a printer in communication with a sender and adapted to receive a print job that has an aspect encrypted with a private key of the sender, to verify the sender by decoding the aspect using a public key of the sender that forms a key pair with the private key, to determine if the sender with the private key has permission to print, and to output the print job only if the aspect of the print job is decoded successfully.

23. (Previously Presented) The printer of claim 22, where the printer is located at a printing site and is further adapted to re-verify the sender by receiving a demonstration that the sender possesses the private key at the printing site.

24. (Original) The printer of claim 23, where printer is adapted to receive the demonstration from a portable processor that stores the private key in memory.

25. (Original) The printer of claim 22, where the aspect relates to content of the print job.

26. (Original) The printer of claim 22, where the aspect, after encryption, is a digital signature.

27. (Original) The printer of claim 22, where the public key is included in a digital certificate.

28. (Original) The printer of claim 22, where the public key is included in the print job.

29. (Original) The printer of claim 22, where the public key is obtained by the printer from a public key database.

30. (Currently Amended) A method for regulating the ability of a user to print on a printer, comprising the steps of:

receiving, at a printer, a print job from a user, where the print job includes a representation of a document and an aspect of the print job that is encrypted with a private key of the user;

verifying the user by decoding the aspect using a public key of the user, where the public key and the private key form a key pair;

determining, in a process distinct from verifying, if the user with the private key has permission to print; and

printing the document on the printer only if the **aspect is decoded successfully and the** user ~~is a verified user and~~ has permission to print.